

April 12, 2021

Via Electronic Mail ([regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov))

Anne E. Misback  
Secretary  
Board of Governors of the Federal Reserve System  
20<sup>th</sup> Street and Constitution Avenue NW  
Washington, DC 20551

**RE: Computer-Security Incident Notification Requirements for Banking Organizations  
and Their Bank Service Providers  
(Docket No. R-1736; RIN 7100-AG06)**

Ladies and Gentlemen:

The Depository Trust & Clearing Corporation (“DTCC”), on behalf of its central securities depository subsidiary, The Depository Trust Company (“DTC”), welcomes the opportunity to provide comments to the Board of Governors of the Federal Reserve System (“Federal Reserve”), the Office of the Comptroller of the Currency (“OCC”), and the Federal Deposit Insurance Corporation (“FDIC”) (collectively, the “Agencies”) in connection with the joint notice of proposed rulemaking that would establish computer-security incident notification requirements for banking organizations and their bank service providers (the “Proposal” or the “Proposing Release”).<sup>1</sup> DTCC understands the Agencies’ rationale in developing the Proposal to ensure they receive timely notice of computer-security incidents that are likely to cause significant harm to individual banking organizations and, potentially, the broader financial system. DTCC submits the following comments to contribute to a final rule that enables the Agencies to achieve their policy goals while minimizing regulatory overlap, duplication, and potential unintended consequences. DTCC respectfully requests that the Agencies take these comments into consideration in finalizing the requirements.

## **A. Overview of DTCC**

DTCC is the parent company and operator of DTC, which is the U.S. central securities depository, and the National Securities Clearing Corporation (“NSCC”) and Fixed Income Clearing Corporation (“FICC”), which are the U.S. cash market securities central counterparties.

---

<sup>1</sup> See FRB, OCC, FDIC, Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers, 86 Fed. Reg. 2299 (January 12, 2021).

DTC, NSCC and FICC are registered under the Securities Exchange Act of 1934, as amended, as clearing agencies. In addition, DTC, NSCC and FICC have been designated as systemically important financial market utilities (“SIFMUs”) by the U.S. Financial Stability Oversight Council (“FSOC”)<sup>2</sup> pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the “Dodd-Frank Act”).<sup>3</sup> In accordance with Title VIII, the U.S. Securities and Exchange Commission (“SEC”) is the Supervisory Agency for DTC, NSCC and FICC. DTC also is licensed as a New York Limited Purpose Trust Company and state member bank of the Federal Reserve System and, as such, is subject to supervision and examination by the New York State Department of Financial Services and the Federal Reserve Bank of New York under delegated authority from the Federal Reserve.

DTCC, through its subsidiaries, is the largest post-trade market infrastructure for the global financial services industry. Given its critical role in the industry, DTCC expends considerable resources each year to safeguard its technology systems and data and defend against threats to prevent incidents. Furthermore, as discussed below, DTCC maintains a mature technology incident management and reporting program to comply with applicable regulatory requirements and established practices.<sup>4</sup> In light of its experience operating SIFMUs and other businesses<sup>5</sup> subjected to a myriad of regulatory frameworks, DTCC offers a unique and valuable perspective in providing comments on the Proposal.

Because DTC would be covered by this definition as a state member bank of the Federal Reserve, DTCC’s comments focus on the proposed Federal Reserve regulations at 12 CFR Part 225, Subpart N (Computer-Security Incident Notification).

## **B. Executive Summary**

The Proposal would require that a banking organization notify the Federal Reserve of any “computer-security incident”<sup>6</sup> that rises to the level of a “notification incident”<sup>7</sup> as soon as

---

<sup>2</sup> See U.S. Department of the Treasury, FSOC Designations, available <https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations> (last visited April 12, 2021).

<sup>3</sup> Pub. L. No. 111-203, 124 Stat. 1376 (2010).

<sup>4</sup> See e.g., SEC Regulation Systems Compliance and Integrity (“Regulation SCI”), 12 CFR 242.1000 – 242.1007.

<sup>5</sup> DTCC also provides services for a significant portion of the global over-the-counter derivatives market. DTCC’s Global Trade Repository services support reporting across all five major derivatives asset classes and exchange-traded derivatives in the U.S., Europe and Asia.

<sup>6</sup> Computer-security incident would mean an occurrence that: (1) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or (2) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Proposed 12 CFR 222.302.

<sup>7</sup> Notification incident would mean a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair— (1) the ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (2) any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value;

possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred (the “Notification Requirement”).<sup>8</sup> The term “banking organization” would include, among other things, a state member bank of the Federal Reserve (each a “Covered Entity” or, collectively, “Covered Entities”).<sup>9</sup>

The Proposal also would require a bank service provider to notify at least two individuals at affected banking organization customers immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided for four or more hours.<sup>10</sup> The term “bank service provider” would mean a bank service company or other person providing services to a banking organization that is subject to the Bank Service Company Act (12 USC 1861-1867) (“BSCA”).<sup>11</sup>

DTCC understands the importance of the Agencies receiving prompt notice of notification incidents to carry out their oversight functions.<sup>12</sup> DTCC offers suggestions and requests clarification regarding certain aspects of the Proposal to maximize its benefits while avoiding regulatory overlap and duplication, and the potential for unintended consequences, such as the creation of separate but parallel incident reporting processes. By way of introduction, DTCC provides the following summary of its comments:

- The Agencies should follow the scope set forth in the Federal Reserve’s Regulation HH by excluding from the Proposal SIFMUs for which the SEC is the Supervisory Agency under Title VIII of the Dodd-Frank Act (“SEC SIFMUs”).
- If the Agencies elect to apply the proposed requirements to SEC SIFMUs, the requirements should be more closely aligned to Regulation SCI.
- The Agencies should change and clarify the proposed requirements in certain important respects, including by incorporating key aspects of the preamble in the rule text and clarifying the scope of the bank service provider definition. In addition, to the extent that the Agencies seek to establish post-notification requirements, protocols, or standards, they should do so through public notice and comment as part of the Agencies’ formal rulemaking processes.

---

or (3) those operations of a banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States. *Id.*

<sup>8</sup> See proposed 12 CFR 225.302.

<sup>9</sup> See proposed 12 CFR 225.301.

<sup>10</sup> See proposed 12 CFR 225.303.

<sup>11</sup> See proposed 12 CFR 225.301.

<sup>12</sup> As described in the Proposal, such incidents may include “major computer-system failures, cyber-related interruptions, such as coordinated denial of service and ransomware attacks, or other types of significant operational interruptions.” Proposing Release, 86 Fed. Reg. at 2301.

By more thoroughly accounting for, and increasing alignment to, existing regulatory reporting frameworks, DTCC believes that the Agencies would reduce regulatory burdens, while creating an effective and efficient regulatory approach.

## **C. Scope of the Proposal**

### **1. Title VIII of the Dodd-Frank Act**

DTCC requests that the Agencies exclude SEC SIFMUs from the Proposal's definition of banking organization. Congress enacted Title VIII to mitigate systemic risk in the financial system and promote financial stability, in part, through enhanced regulation and supervision of SIFMUs.<sup>13</sup> Title VIII authorizes the Supervisory Agency of a SIFMU, in consultation with the Federal Reserve and FSOC, to prescribe risk management standards for that SIFMU.<sup>14</sup> As set forth in Title VIII, the SEC is the Supervisory Agency for a SIFMU that is an SEC-registered clearing agency and the Federal Reserve is the Supervisory Agency for a SIFMU that is otherwise not covered by another agency.<sup>15</sup>

Under this framework, the SEC is the Supervisory Agency for DTC, and DTC is subject to the SEC's Standards for Covered Clearing Agencies.<sup>16</sup> In the proposing release to Regulation HH, the Federal Reserve acknowledged that Title VIII grants the SEC authority to prescribe risk management standards for SEC SIFMUs and, in recognition that SEC SIFMUs would be subject to the risk management standards promulgated by the SEC, proposed that Regulation HH would not apply to these entities.<sup>17</sup> The Federal Reserve ultimately adopted this exclusion and, accordingly, DTC is not subject to the requirements of Regulation HH.<sup>18</sup> By natural extension,

---

<sup>13</sup> See 12 USC 5461.

<sup>14</sup> See 12 USC 5464. Under this section of the Dodd-Frank Act, rulemaking by the SEC and CFTC must be done in consultation with the Federal Reserve and FSOC and take into consideration relevant international standards and existing prudential requirements. 12 USC 5464(a)(2). In addition, Title VIII provides for enhanced coordination between the SEC and the Federal Reserve by allowing for regular examinations and information sharing. See 12 U.S.C. 5466.

<sup>15</sup> See 12 USC 5462(8)(A).

<sup>16</sup> See generally, 17 CFR § 240.17Ad-22(e). The statutory objectives and principles for these risk management standards are to promote robust risk management, promote safety and soundness, reduce systemic risks, and support the stability of the broader financial system. See 12 USC 5464(b).

<sup>17</sup> See Federal Reserve, Financial Market Utilities, 76 Fed. Reg. 18445, 18448 (April 4, 2011). See also Federal Reserve, Financial Market Utilities, 79 Fed. Reg. 3666, 3666-67 (January 22, 2014) (proposed amendments to the risk management standards in Regulation HH to incorporate the Principles for Financial Market Infrastructures, which recognized and continued the exclusion for SEC SIFMUs).

<sup>18</sup> See 12 CFR 234.1(b) ("The risk management standards do not apply, however, to a designated financial market utility that is a derivatives clearing organization registered under section 5b of the Commodity Exchange Act (7 U.S.C. 7a-1) or a clearing agency registered with the Securities and Exchange Commission under section 17A of the Securities Exchange Act of 1934 (15 U.S.C. 78q-1), which are governed by the risk-management standards promulgated by the Commodity Futures Trading Commission or the Securities and Exchange Commission, respectively, for which each is the Supervisory Agency.").

the SEC's role as the primary rulemaking authority for SEC SIFMUs should be respected in connection with the development of incident management and reporting standards. This is especially true in an area where, as in the case of Regulation SCI, the SEC already established robust and effective regulatory requirements. The SEC adopted Regulation SCI to "address the technological vulnerabilities, and improve Commission oversight, of the core technology of key U.S. Securities markets entities," including SEC SIFMUs.<sup>19</sup> Among other obligations, Regulation SCI requires immediate notification to the SEC upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred.<sup>20</sup> The term SCI event broadly includes systems disruptions, systems compliance issues, and systems intrusions, as those terms are defined in Regulation SCI.<sup>21</sup>

With Regulation SCI's extensive requirements in place, it is unnecessary and potentially duplicative to subject SEC SIFMUs, including DTC, to a different regulatory framework that is designed to achieve the same outcomes outlined in the Proposal. Instead, the Federal Reserve should adopt a parallel approach to Regulation HH in establishing technology incident management and reporting standards and defer to SEC regulatory requirements for SEC SIFMUs.<sup>22</sup> Such an approach is consistent with congressional intent regarding the enhanced regulation and supervision of SIFMUs set forth in Title VIII, and avoids unintended regulatory overlap and duplication and the potential burden of compliance with different requirements to achieve the same purpose.

---

<sup>19</sup> SEC, Regulation Systems Compliance and Integrity, 79 Fed. Reg. 72252, 72253 (December 5, 2014) ("Regulation SCI adopting release"). See 17 CFR 242.1000 (definition of "SCI entity"). See also SEC, Standards for Covered Clearing Agencies, Exchange Act Release No. 34-78961, 81 Fed. Reg. 70786 (Oct. 13, 2016) (noting that "Regulation SCI is designed to reduce the occurrence of systems issues, improve resiliency when systems problems do occur, and enhance the [SEC's] oversight and enforcement of securities market technology infrastructure. Since adoption of Regulation SCI, the [SEC] has established a monitoring and examination structure to oversee compliance with Regulation SCI.").

<sup>20</sup> 17 CFR 242.1002(b). The term responsible SCI personnel means, for a particular SCI system or indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s). 17 CFR 242.1000.

<sup>21</sup> See 17 CFR 242.1000. More specifically, the terms are defined as follows: systems compliance issue means an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable; systems disruption means an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system; and systems intrusion means any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity. *Id.*

<sup>22</sup> The Agencies' goals for the Proposal should be considered in light of congressional allocation of rulemaking authority under Title VIII as well as the burdens of imposing overlapping and duplicative requirements on Covered Entities already subject to similar existing regulatory frameworks. More generally, for Federal Reserve proposals to establish regulatory requirements that would apply to SEC SIFMUs, DTCC encourages a regulatory approach that recognizes the SEC's status as Supervisory Agency under Title VIII.

## **2. Alignment of the Policy Goals of Regulation SCI and the Proposal**

The Agencies state that the Notification Requirement is intended to serve as an early alert to the Agencies, as applicable, and is not intended to provide an assessment of the incident.<sup>23</sup> The Agencies further state that:

The agencies believe that it is important that the primary federal regulator of a banking organization be notified as soon as possible of a significant computer-security incident that could jeopardize the viability of the operations of an individual banking organization, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector.<sup>24</sup>

DTCC supports the purpose of the Proposal and agrees with the Agencies' statement about the importance of timely notice to and effective oversight by supervisory authorities. From a practical perspective, however, DTC already satisfies the Proposal's goals through its existing technology incident management and reporting program, which is structured to comply with the reporting requirements of Regulation SCI.

As described above, Regulation SCI includes stringent notification requirements. Based on DTCC's analysis of the Proposal as compared to Regulation SCI, any incident triggering the Notification Requirement, as modified by the suggestions below, would be covered by Regulation SCI's immediate reporting requirement. DTC's long-standing practice is to promptly notify its regulators, as appropriate and in accordance with supervisory expectations, of significant technology incidents.<sup>25</sup> For these reasons, DTCC believes its existing process for identifying and reporting technology incidents to comply with applicable regulatory requirements and established practices already achieves the Agencies' policy goals as set forth in the Proposal. Thus, following the approach set forth in section C.1. above would not impede the policy goals identified in the Proposal. On the other hand, requiring DTC to comply with the requirements set forth in the Proposal would necessitate the creation of separate but parallel processes, which risks introducing unnecessary operational complexities at precisely the time at which it should be focused on addressing the incident.

The Agencies state in the Proposal that they "considered whether incident reporting under the Proposal could be obtained through existing reporting standards."<sup>26</sup> While the Agencies considered certain existing regulations and guidance in connection with formulating the Proposal,<sup>27</sup> the Agencies did not appear to consider other key regulatory frameworks that impose

---

<sup>23</sup> Proposing Release, 86 Fed. Reg. at 2303.

<sup>24</sup> Id. at 2301 (footnote omitted).

<sup>25</sup> As the Agencies acknowledge, the Proposal largely "would formalize a process that already exists, based on the [A]gencies' experiences." Id. at 2304.

<sup>26</sup> Id. at 2301. Ultimately, the Agencies concluded that "current reporting requirements related to cyber incidents are neither designed nor intended to provide timely information to regulators regarding such incidents." Id.

<sup>27</sup> See id. This discussion reviews reporting requirements of the Bank Secrecy Act (31 USC 5311 et seq.) and its implementing regulations; supervisory expectations set forth in the Interagency Guidance on Response Programs for

significant technology incident reporting obligations on Covered Entities, including Regulation SCI.<sup>28</sup> DTCC urges the Agencies to carefully consider these applicable regulatory frameworks before imposing additional requirements on Covered Entities. By doing so, the Agencies may conclude there are effective alternatives, such as the approach set forth in section C.1. above, to achieve their policy goals with the Proposal.

### **3. Regulation SCI as an Alternative Means of Compliance with the Proposal**

As stated above, SEC SIFMUs should be removed from the scope of the Proposal to avoid regulatory overlap, duplication and potentially conflicting requirements in relation to Regulation SCI. As an alternative approach, the Federal Reserve could incorporate into the Proposal a provision stating that Covered Entities subject to Regulation SCI shall be deemed in compliance with the Federal Reserve's final rule (once adopted). This alternative approach would avoid the need for SEC SIFMUs to establish separate but parallel technology incident management and reporting programs for purposes of Regulation SCI and the Proposal.

### **D. Increased Alignment of the Proposal to Regulation SCI**

DTCC is concerned that a continued proliferation of technology incident management and reporting requirements will introduce regulatory overlap, duplication, and potentially inconsistent requirements as applied to Covered Entities subject to multiple regulatory frameworks. If the Agencies conclude that SEC SIFMUs should be included within the scope of the Proposal and decline to adopt the alternative compliance means detailed above, DTCC suggests that the Agencies modify the Proposal to be more closely aligned to Regulation SCI. Improving the Proposal's alignment to existing standards and requirements will improve its effectiveness and enhance the Agencies' ability to achieve their policy goals. Below DTCC suggests several modifications of the Proposal to improve its alignment to existing standards and requirements.

#### **1. Definition of Computer-Security Incident**

The Proposal defines a computer-security incident as an occurrence that either (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.<sup>29</sup> DTCC requests that the Agencies narrow this definition to focus on actual incidents, which is consistent with the goal of the Proposal to require reporting of incidents "likely to cause significant harm to banking organizations."<sup>30</sup> More specifically, the Agencies

---

Unauthorized Access to Customer Information and Customer Notice (see e.g., 12 CFR Part 208, Appendix D-2); and notification requirements of the Bank Service Company Act (12 USC 1867(c)(2)).

<sup>28</sup> An additional existing regulation that warrants consideration is the New York State Department of Financial Services' cybersecurity requirements for financial services companies (23 NYCRR 500).

<sup>29</sup> Proposed 12 CFR 225.301.

<sup>30</sup> Proposing Release at 2305.

should strike the words “or potential” in the first prong of the definition because a potential harm reasonably cannot be expected to trigger the Notification Requirement. The Agencies also should delete the second prong of the definition in its entirety because it would cover a high volume of insignificant incidents and any meaningful incident already would be captured under the first prong of the definition.<sup>31</sup> Accordingly, DTCC recommends that the Agencies adopt the following definition:

*Computer-security incident* is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

DTCC understands that the Agencies sought to align the definition of computer-security incident to the term’s existing definition from the National Institute of Standards and Technology (“NIST”).<sup>32</sup> DTCC commends the Agencies’ effort to leverage NIST standards and, in general, DTCC supports the use of a common lexicon of terminology across the financial industry to foster effective communication and increased understanding of regulatory requirements. In the context of the Proposal, however, an overly broad definition of computer-security incident will require Covered Entities to analyze a high volume of potential yet unrealized incidents to determine whether each occurrence rises to the level of a notification incident.<sup>33</sup> For larger Covered Entities, this could result in analyzing a substantial number of immaterial incidents to determine whether they meet a reporting threshold when the reporting ultimately will not yield any meaningful benefit because those incidents cause no disruption or other impact. For these reasons, DTCC recommends that the definition of computer-security incident be drawn as narrowly as possible to ensure the efficient and effective use of Agency and Covered Entity resources.

More broadly, DTCC encourages the Agencies and other policymakers to be cognizant of the important distinction between incidents and events when establishing technology incident reporting requirements. Whereas all incidents are events, not all events are incidents. An event may or may not rise to the level of an incident and could be viewed as one in a series of breadcrumbs leading to an actual incident. A few illustrative examples are below:

- A security patch not applied past the remediation timeframe may be a policy violation event; if the vulnerability is not exploited, however, it is not an incident.

---

<sup>31</sup> For example, most organizations have timeframes for the patching of vulnerable systems. In some cases, these patches cannot be implemented in the timeframe allotted (e.g., managed hardware devices from third parties; certain versions of commercial off-the-shelf products). Technically, the missing patch may be a policy violation. While the missing patch is not desirable, it would not be considered an incident. Rather, it would be an event that, if in sufficient number, may be outside the organization’s risk tolerance.

<sup>32</sup> Proposing Release at 2300, n.3. See NIST, Computer Security Resource Center, Glossary: Computer Security Incident, available at [https://csrc.nist.gov/glossary/term/Computer\\_Security\\_Incident](https://csrc.nist.gov/glossary/term/Computer_Security_Incident) (last visited February 9, 2021).

<sup>33</sup> Certain unrealized incidents, such as unsuccessful systems intrusion attempts, demonstrate that a Covered Entity’s systems are adequately protected. Reporting such incidents would be inconsistent with the Agencies’ stated goal with the Proposal to receive timely notice of incidents “likely to cause significant harm” to Covered Entities. Proposing Release, 86 Fed. Reg. at 2305.

- If a business application is not able to meet the complex password requirements, it may be a policy violation event, but it is not an incident.
- If a firewall drops connections that it is not configured to pass or a user incorrectly enters a password, there may be an event but not an incident. Continuing with these examples, if the firewall gets flooded to the point where it cannot handle legitimate requests or there are numerous incorrect logins for multiple accounts that simultaneously lock all users out of the system, then these are incidents because they result in actual impacts.

The distinction between incidents and events has implications in global discussions on incident reporting frameworks because at times these terms are used interchangeably, and may have a significant impact on the activities that must be reported. As described above, DTCC believes that only those events that create actual harm should be considered incidents.

## 2. Scope of Covered Information Systems

The Proposal's definition of computer-security incident relates to incidents involving "an information system, or the information that the system processes, stores, or transmits."<sup>34</sup> DTCC requests that the Agencies limit the scope of this general reference to "information system" by requiring in the definition of a notification incident a direct nexus between the system and the Covered Entity, as shown below (additions are underlined; deletions are marked with strikethrough):

*Notification incident* is a computer-security incident involving an information system operated by, or on behalf of, a banking organization and ~~that a~~ the banking organization believes in good faith could materially disrupt, degrade, or impair—  
....

DTCC believes this change to the definition of notification incident is necessary because it would be unduly burdensome and potentially unrealistic for Covered Entities to be accountable for compliance with the Notification Requirement with respect to systems operated by third parties that have an attenuated or indirect relation to a Covered Entity's core banking systems. For example, with respect to incidents involving third party systems that do not directly support a Covered Entity's core banking systems, the Covered Entity would not necessarily have access to information sufficient to meet the Agencies' expectations under the Proposal. This change also would improve alignment with the scope of systems covered by Regulation SCI.<sup>35</sup>

---

<sup>34</sup> Proposed 12 CFR 225.301.

<sup>35</sup> See Regulation SCI adopting release, *supra* note 19, 79 Fed. Reg. at 72276 (stating that the term SCI systems includes a system operated on behalf of an SCI entity).

### **3. “Believes in Good Faith” Standard**

The Notification Requirement would be triggered once a Covered Entity believes in good faith that a notification incident has occurred.<sup>36</sup> DTCC is concerned that imposing the “believes in good faith” standard at the entity level will present practical challenges in any reasonably-sized organization. At this level, an undefined number of personnel, including low-level employees and potentially even third parties, could be implicated in the determination of whether an entity has formed a belief that triggers the Notification Requirement. DTCC suggests modifying the Proposal to contemplate the designation by Covered Entities of appropriate individual personnel with responsibility to make appropriate regulatory determinations. Under this modified approach, Covered Entities would establish a process to identify and escalate incidents to appropriately senior personnel empowered to determine whether an incident triggers the Notification Requirement. In addition, Covered Entities would have flexibility to identify the appropriately senior personnel who are authorized to take the necessary actions under the regulations and train such designated personnel to understand their responsibilities. This modified approach also would be consistent with the requirements of Regulation SCI.<sup>37</sup>

Further, it is unclear how the “believes in good faith” standard relates to other existing regulatory reporting standards such as Regulation SCI, which applies a “reasonable basis to conclude” standard. The Proposal’s approach introduces a subjective standard that raises questions about what level of knowledge constitutes a belief for purposes of the reporting obligation. To address these concerns, DTCC suggests that the Agencies modify the Proposal by applying a “reasonable basis to conclude” standard at the level of designated personnel.

#### **E. Recommended Changes and Requests for Clarification**

DTCC appreciates the principles-based nature of the requirements and standards set forth in the Proposal. DTCC emphasizes the importance of flexible, risk-based, outcome-focused rulemaking because it enables each regulated entity to tailor and focus its efforts based on its business model, operational capabilities and infrastructure, and risk profile. This approach results in more effective regulation and improves the likelihood that policymakers will achieve their policy goals. With these principles in mind, DTCC recommends that the Agencies make certain changes and clarifications to the Proposal as described below.

---

<sup>36</sup> Proposed 12 CFR 225.302.

<sup>37</sup> Regulation SCI requires the designation of “responsible SCI personnel” and triggers reporting requirements upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. 17 CFR 242.1001(c), 242.1002(b).

## **1. Incorporate Certain Key Aspects of the Preamble in the Rule Text**

### **a. Reportable Incident Categories and Examples**

The purpose of the Proposal is to make sure that Covered Entities provide timely notice of significant computer-security incident disruptions to the Agencies.<sup>38</sup> The intended scope of the Notification Requirement is informed by the Agencies' identification of several categories<sup>39</sup> and specific examples of reportable incidents.<sup>40</sup> In DTCC's view, the cited categories and examples of notification incidents are consistent with the Agencies' statement that the Notification Requirement is focused "only on events that are likely to cause significant harm to banking organizations."<sup>41</sup> Nevertheless, this stated intent is not clearly evident in the rule text. It is important to recognize that the degree of impact of certain types of incidents may vary across the broad spectrum of entities covered by the Proposal. DTCC is concerned that without more in the rule text to bring the notification incident definition closer to its intended scope, the proposed definition may have the unintended consequence of triggering the Notification Requirement for minor incidents that occur in the normal course of business for certain entities. Notifications of minor incidents could frustrate the Agencies' goals and impair supervisory oversight by, among other things, masking critical incidents and diverting valued resources at Covered Entities and the Agencies.

To improve the alignment of the notification incident definition to its intended scope, DTCC recommends that the Agencies incorporate or otherwise reference in the rule text the categories and examples of notification incidents listed in the Proposing Release.<sup>42</sup> The Agencies could also enhance the materiality standard in the definition so that only genuinely disruptive incidents are captured.

---

<sup>38</sup> Proposing Release, 86 Fed. Reg. at 2301.

<sup>39</sup> See *supra* note 12.

<sup>40</sup> See Proposing Release, 86 Fed. Reg. at 2302. The examples include large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., more than 4 hours); a bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable; a failed system upgrade or change that results in widespread user outages for customers and bank employees; an unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan; a computer hacking incident that disables banking operations for an extended period of time; malware propagating on a banking organization's network that requires the banking organization to disengage all internet-based network connections; and a ransom malware attack that encrypts a core banking system or backup data. *Id.* By contrast, a limited distributed denial of service attack that is promptly and successfully managed by a Covered Entity would not meet the definition of a notification incident. *Id.*

<sup>41</sup> *Id.* at 2305.

<sup>42</sup> See *supra* notes 12 and 40.

## **b. Timing and Content of Required Notifications**

Under the Notification Requirement, a Covered Entity must notify the applicable agency of a notification incident as soon as possible and no later than 36 hours after the entity believes in good faith that a notification incident has occurred.<sup>43</sup> The rule text does not provide any further indication of the intended timing or content of the Notification Requirement. The Proposing Release does, however, contain the following discussion:

The agencies do not expect that a banking organization would typically be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. Rather, the agencies anticipate that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident. In this context, the agencies recognize banking organizations may not come to a good faith belief that a notification incident has occurred outside of normal business hours. Only once the banking organization has made such a determination would the requirement to report within 36 hours begin.<sup>44</sup>

This statement is helpful in understanding the Agencies' intended approach with the Notification Requirement, but it conflicts with the rule text. A plain reading of the rule text's "as soon as possible and" language suggests that notification is required immediately, with 36 hours as the backstop by which the notification must be received by the Agencies. DTCC understands that an immediate timing standard is not intended by the Agencies.<sup>45</sup> To address this discrepancy, DTCC suggests that the Agencies eliminate the words "as soon as possible and" from the rule text. This suggestion also would avoid the ambiguity and related uncertainty presented by the inclusion of "as soon as possible" in the timing standard of the Notification Requirement.

In addition, the Agencies' intended standards for the content of a notice under the Notification Requirement is unclear. The rule text is silent on this issue. In the Proposing Release, the Agencies repeatedly state that such notice is not intended to include an assessment of the incident.<sup>46</sup> The Agencies further state that "no specific information is required for the notice, and the proposed rule does not include any prescribed reporting forms or templates to minimize reporting burden."<sup>47</sup> Covered Entities would be expected only to share "general

---

<sup>43</sup> Proposed 12 CFR 225.302.

<sup>44</sup> Proposing Release, 86 Fed. Reg. at 2302.

<sup>45</sup> DTCC's understanding is based its review of the Agencies' statements in the Proposing Release. For example, the Agencies state their belief that "36 hours is a reasonable amount of time" for notice to the applicable agency. *Id.* at 2303.

<sup>46</sup> See *id.* at 2300, 2303.

<sup>47</sup> *Id.* at 2303.

information about what is known at the time.”<sup>48</sup> Given the importance of these statements to understanding the content standards of the Notification Requirement, DTCC requests that the Agencies incorporate them into rule text. In doing so, consistent with the Agencies’ discussion in the preamble, DTCC encourages the Agencies to preserve flexibility for Covered Entities in the final rule regarding the form and substance of notifications under the Notification Requirement. DTCC also encourages the Agencies to allow for notification through multiple communication channels, including email, telephone, and other technological means, as described in the rule text.<sup>49</sup>

### **c. Confidential Treatment**

DTCC supports the Agencies’ statement in the Proposal that any information provided by a Covered Entity relating to an incident notification would be subject to the Agencies’ confidentiality rules. This treatment is appropriate given the highly sensitive nature of the business, regulatory and security information that would be provided under the Notification Requirement.

## **2. Clarify the Scope of “Bank Service Provider”**

Under the Proposal’s bank service provider notification requirement, a bank service provider would be required to notify affected banking organization customers immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair the provision of services subject to the BSCA.<sup>50</sup> The Proposal would define a bank service provider as a bank service company or other person providing services to a banking organization that is subject to the BSCA.<sup>51</sup> The Agencies state that the bank service provider notification requirement would include both bank service companies and third-party providers under the BSCA.<sup>52</sup> DTCC understands that the services covered in the definition of Bank service provider are those services that are covered by the BSCA. However, DTCC is concerned that the scope of the proposed definition of bank service provider could be misconstrued due to the order of its component parts. To address the concern, DTCC recommends that the Agencies modify the definition of bank service company to provide as follows (additions are underlined; deletions are marked with strikethrough):

---

<sup>48</sup> Id. The Agencies assert that “the regulatory burden associated with the notice requirement would be de minimis[] because the communications that led to the determination of the notification incident would occur regardless of the proposed rule.” Id. at 2305.

<sup>49</sup> See proposed 12 CFR 225.302 (allowing for “any form of written or oral communication, including through any technological means (*e.g.*, email, telephone, text, etc.)....”). See also Proposing Release, 86 Fed. Reg. at 2303 (“[N]otice could be provided through any form of written or oral communication, including through any technological means (*e.g.*, email or telephone)....”).

<sup>50</sup> See proposed 12 CFR 225.303.

<sup>51</sup> See proposed 12 CFR 225.301(a); see also 12 USC 1861-1867.

<sup>52</sup> Proposing Release, 86 Fed. Reg. 2301, n.6.

Bank service provider means a bank service company or other person providing services, as defined in the Bank Service Company Act (12 U.S.C. 1861–1867) (“BSCA”), to a banking organization that is subject to the BSCA ~~Bank Service Company Act (12 U.S.C. 1861–1867)~~.

As an alternative approach, the Agencies should clarify in the rule text that the definition is making reference to permissible services under the BSCA, which must be permissible for a company under section 1843(c)(8) of the Bank Holding Company Act of 1956,<sup>53</sup> as amended, and section 225.28 of the Federal Reserve’s Regulation Y.<sup>54</sup>

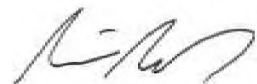
### **3. Provide Standards, Requirements and Expectations for Covered Entities following Notification as Part of the Rulemaking Process**

The Proposal focuses on standards and requirements relating to the notification of a reportable incident to the Agencies. The Proposal is silent, however, on the Agencies post-notification activities and expectations for Covered Entities. The Proposal merely states that the Agencies may provide additional guidance in the future.<sup>55</sup> To the extent that the Agencies seek to establish post-notification requirements, protocols, or standards, DTCC believes that the Agencies should do so through public notice and comment as part of the Agencies’ formal rulemaking processes.

#### **F. Conclusion**

DTCC appreciates the opportunity to provide comments on the Proposal and your consideration of the views expressed in this letter. DTCC welcomes the opportunity for further discussions and engagement on the topics raised in this letter. If you have any questions or need further information, please contact me at (212) 855-4844 or [sscharf@dtcc.com](mailto:sscharf@dtcc.com).

Sincerely,



Stephen Scharf  
Managing Director and Global Chief Security Officer  
DTCC

---

<sup>53</sup> See 12 USC 1841, et seq.

<sup>54</sup> 12 CFR 225.28 (Activities permissible under this section are (1) extending credit and servicing loans; (2) activities related to extending credit; (3) leasing personal or real property; (4) operating nonbank depository institutions; (5) trust company functions; (6) financial and investment advisory activities; (7) agency transactional services for customer investments; (8) investment transactions as principal; (9) management consulting and counseling activities; (10) support services; (11) insurance agency and underwriting; (12) community development activities; (13) money orders, savings bonds, and traveler’s checks; and (14) data processing).

<sup>55</sup> Proposing Release, 86 Fed. Reg. at 2304.